

Michael Connett (SBN 283360)
SIRI & GLIMSTAD LLP
700 S. Flower Street, Ste. 1000
Los Angeles, CA 90017
Telephone: (772) 783-8436
mconnett@sirillp.com

Tyler J. Bean*
Sonjay C. Singh*
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (772) 783-8436
tbean@sirillp.com
ssingh@sirillp.com

**UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF CALIFORNIA**

**M.S. AND C.P., ON BEHALF OF
THEMSELVES AND ALL OTHERS
SIMILARLY SITUATED,**

Plaintiff,

vs.

**AYLO GLOBAL ENTERTAINMENT,
INC., AYLO USA INCORPORATED,
AND TOQON, LLC D/B/A
TRAFFICJUNKY.**

Defendants.

**Civil Action No.: 2:25-cv-01139-DJC-
JDP**

**SECOND AMENDED CLASS
ACTION COMPLAINT**

Plaintiffs M.S. and C.P., (collectively, "Plaintiffs"), individually and on behalf of all similarly situated persons, allege the following against Defendants Aylo Global Entertainment, Inc., Aylo USA Incorporated (collectively, "Pornhub") and Toqon, LLC

d/b/a TrafficJunky (“TrafficJunky” and together with Pornhub, “Defendants”) based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation by Plaintiffs’ counsel and review of public documents as to all other matters:

I. INTRODUCTION

1. A person’s sexual desires are some of the most sensitive, personal things in life. As the Supreme Court has stated, an individual’s sexual behavior within their own home represents the “most private human conduct...in the most private of places.” *Lawrence v. Texas*, 539 U.S. 558, 567 (2003).

2. For a majority of Americans, their sexual lives in some way involve viewing pornography. Even though the statistics vary, a 2020 academic study reported that “[u]sing all modalities of pornography, 91.5% of men and 60.2% of women herein reported having consumed pornography in the past month.”¹ Likewise, according to a 2023 research article reported on in Psychology Today:

Using a set of metrics that includes indicators of monthly unique visitors as well as monthly pageviews, the authors [of the article in the Journal Of Sex Research] found that the top three pornography sites are more highly ranked than the most well-known household name sites (Amazon, Netflix, Yahoo) as well as those that are the most up and coming (TikTok, OpenAI/ChatGPT, Zoom).²

¹ Solano, Eaton & O’Leary, *Pornography Consumption, Modality and Function in a Large Internet Sample* (J. Sex Res. Jan. 2020) available at <https://pubmed.ncbi.nlm.nih.gov/30358432/>

² McNichols, Nicole K. Ph.D., *How Many People Actually Watch Porn?* (Psychology Today Sept. 25, 2023) available at <https://www.psychologytoday.com/us/blog/everyone-on-top/202309/how-much-porn-do-americans-really-watch> (reporting on Wright, Tokunaga & Herbenick, *But Do Porn Sites Get More Traffic than TikTok, OpenAI, and Zoom?*, 763-767 (J. Sex Res. June 5, 2023) available at <https://www.tandfonline.com/doi/full/10.1080/00224499.2023.2220690>)

1 That result is consistent with a similar study performed a decade earlier, which found that
2 pornography sites were unquestionably the most popular on the internet.

3 3. Yet despite its prevalence, pornography usage is still something people do
4 not discuss. For example, a large percentage of couples in a 2021 study reported that their
5 significant other does not know the frequency of pornography that they watch.³ It is not
6 surprising that people want to keep their pornography usage to themselves, as many
7 people still disapprove of it and the effects it can have on participants and relationships.⁴
8 Thus, it is clear that pornography usage is an extremely private thing that while most
9 people do it, they do not want anyone to know about it.

10 4. Pornhub is one of the most popular pornography destinations on the
11 internet. It hosts a wide range of pornographic content including millions of pornographic
12 videos.⁵ It alone is the nineteenth most-visited website on the entire Internet, with its
13 Website—www.pornhub.com (the “Website”)—receiving *billions* of visits each year.⁶

14 5. Plaintiffs used The Website to privately view pornographic media from the
15 comfort of their own homes. Given how confidential the entire subject is, when Plaintiffs
16 used the Website, they assumed that Pornhub would do its utmost to keep their use of its
17 service private.

18
19 ³ Crawford & Butler, *The Truth Hurts Less: Pornography Use Disclosure vs. Deception* (Inst. for
20 Family Stud. July 7, 2021) available at [https://ifstudies.org/blog/the-truth-hurts-less-pornography-use-](https://ifstudies.org/blog/the-truth-hurts-less-pornography-use-disclosure-vs-deception)
21 [disclosure-vs-deception](https://ifstudies.org/blog/the-truth-hurts-less-pornography-use-disclosure-vs-deception) (“In a nationally representative study of couples in committed relationships,
22 37% of men reported more pornography use than their partner believed was occurring. In casually
dating relationships, 43% of the men reported using pornography daily or every other day, while none
of their partners reported awareness of that level of use.”)

23 ⁴ Carroll & Willoughby, *The Porn Gap: Gender Differences in Pornography Use in Couple*
24 *Relationships* (Inst. for Family Stud. Oct. 5, 2017) available at [https://ifstudies.org/blog/the-porn-gap-](https://ifstudies.org/blog/the-porn-gap-gender-differences-in-pornography-use-in-couple-relationships)
25 [gender-differences-in-pornography-use-in-couple-relationships](https://ifstudies.org/blog/the-porn-gap-gender-differences-in-pornography-use-in-couple-relationships).

26 ⁵ Zoe Haylock, *Pornhub Just Deleted Most of Its Content*, VULTURE (Dec. 14, 2020),
27 <https://www.vulture.com/2020/12/pornhub-deletes-all-unverified-content-millions-of-videos.html>
(last visited Apr. 16, 2025).

28 ⁶ *Top Websites*, SIMILARWEB (Feb. 2025), <https://www.similarweb.com/top-websites/> (last visited
Apr. 16, 2025).

1 6. Unfortunately, unbeknownst to Plaintiffs and other visitors to the Website,
2 Pornhub does not keep sensitive information about their Website visitors private. Instead,
3 Defendants collect and transmit information related to individuals' use of the Website,
4 including the specific pornographic videos that they watch (the "Sensitive Information"),
5 to third party advertisers, including Alphabet Inc. ("Google"), through the use of
6 surreptitious online tracking tools.

7 7. Online advertising giants, like Google, try to compile as much information
8 as possible about American consumers, including the most private aspects of their lives,
9 as fuel for a massive, targeted advertising enterprise. Any information about a person
10 captured by those online behemoths can be used to stream ads to that person. If Google
11 receives information that a person views pornography, it will use that information, and
12 allow its clients to use that information, to stream ads to that person's computers and
13 smartphones relating to the specific types of pornography that the person consumes.

14 8. Google offers website operators access to its proprietary suites of
15 marketing, advertising, and customer analytics software, including Google Analytics,
16 Google AdSense, and Google Tag Manager (collectively, the "Business Tools"). Armed
17 with these Business Tools, website operators can leverage Google's enormous database
18 of consumer information for the purposes of deploying targeted advertisements,
19 performing minute analyses of their customer bases, and identifying new market segments
20 that may be exploited.

21 9. But, in exchange for access to these Business Tools, website operators
22 install Google's surveillance software on their website (the "Google Tracking Tools"),
23 including 'tracking pixels' ("Pixels") and third-party 'cookies' that capture sensitive,
24 personally identifiable information provided to the website operator by its website users.
25 This sensitive information can include a unique identifier that Google uses to identify that
26 user, regardless of what computer or phone is used to access the website. The Google
27

1 Tracking Tools can also capture and share other information like the specific webpages
2 visited by a website user, items added to an online shopping cart by a website user,
3 information entered into an online form by a website user, and the device characteristics
4 of a website user's phone or computer.

5 10. In essence, when website operators use Google's Business Tools, they
6 choose to participate in Google's mass surveillance network and, in turn, benefit from
7 Google's collection of user data at the expense of their customers' privacy.

8 11. Pornhub chose to accept the devil's bargain offered by Google by installing
9 the Google Tracking Tools on the Website.

10 12. But, Pornhub's surveillance of its users is not only accomplished through
11 use of Google's Tracking Tools but also through TrafficJunky's surveillance software
12 suite (the "TrafficJunky Tracking Tools", and together with the Google Tracking Tools,
13 the "Tracking Tools"), which collects information from the Website and other websites
14 operated by Pornhub, correlates that information with information collected through the
15 Google Tracking Tools, and allows for even more detailed tracking of Website users'
16 pornography consumption.

17 13. Each of the Plaintiffs and Class Members visited the Website and had their
18 personal Sensitive Information tracked by Defendants using the Tracking Tools.
19 However, Defendants *never* obtained informed consent from Plaintiffs or Class Members
20 to share the Sensitive Information it collects with third parties, let alone with Google, the
21 largest advertiser and compiler of user information in the world.

22 14. Moreover, Defendants' tracking of Website users violated numerous state
23 and federal laws, including the Video Privacy Protection Act ("VPPA"), passed
24 specifically to prevent the disclosure and aggregation of data relating to an individual's
25 video consumption.

16. Therefore, Plaintiffs seek, on behalf of themselves and a class of similarly situated persons, to remedy these harms and assert the following statutory and common law claims against Defendant: Invasion of Privacy; Breach of Confidence; Negligence; Breach of Implied Contract; violations of the Video Privacy Protection Act (“VPPA”), 18 U.S.C. § 2710, *et seq.*; violations of the Electronic Communications Privacy Act (“ECPA”); violations of N.Y. Gen. Bus. Law § 349; violations of the California Invasion of Privacy Act (“CIPA”); Cal. Pen. Code § 360, *et seq.*; and violations of the California Unfair Competition Law (“UCL”), Cal. Bus. & Prof. Code, § 17200, *et seq.*

16 ***Plaintiff M.S.***

17 17. Plaintiff M.S. is a citizen of the state of California, residing in El Dorado
18 County, and brings this action both in an individual capacity, and on behalf of all others
19 similarly situated.

18. Plaintiff M.S. registered for an account on the Website and utilized it on his personal electronic devices on multiple occasions in 2024 and 2025, to view pornographic media, including paid content.

19. Unbeknownst to Plaintiff M.S., The Tracking Tools contemporaneously transmitted the Sensitive Information that was communicated to and from Plaintiff M.S. as he used the Website, including the specific videos that he viewed.

20. Plaintiff M.S. never authorized Defendants to disclose any aspect of his communications with Defendants through the Website to third parties.

21. On every occasion that he visited The Website, Plaintiff M.S. possessed an account with Google, and he accessed The Website while logged into his Google account on the same device.

Plaintiff C.P.

22. Plaintiff C.P. is a citizen of the state of New York, residing in Richmond County, and brings this action both in an individual capacity, and on behalf of all others similarly situated.

23. Plaintiff C.P. registered for an account on the Website and utilized it on his personal electronic devices on multiple occasions in 2024 and 2025, to view pornographic media.

24. Unbeknownst to Plaintiff C.P., The Tracking Tools contemporaneously transmitted the Sensitive Information that was communicated to and from Plaintiff C.P. as he used the Website, including the specific videos that he viewed.

25. Plaintiff C.P. never authorized Defendants to disclose any aspect of his communications with Defendants through the Website to third parties.

26. On every occasion that he visited The Website, Plaintiff C.P. possessed an account with Google, and he accessed The Website while logged into his Google account on the same device.

Defendant Aylo Global Entertainment, Inc.

27. Defendant Aylo Global Entertainment, Inc. is a limited liability corporation incorporated in Delaware with its principal place of business at 610 Brazos St, Suite 500 Austin, Texas 78701. Defendant Aylo Global Entertainment, Inc. operates the Website.

Defendant Aylo Usa Incorporated

28. Defendant Aylo USA Incorporated is a limited liability corporation incorporated in Delaware with its principal place of business at 610 Brazos St, Suite 500 Austin, Texas 78701. Defendant Aylo USA Incorporated operates the Website.

Defendant Toqon LLC

29. Defendant Toqon LLC is a limited liability corporation incorporated in Delaware with its principal place of business at 610 Brazos St, Suite 500 Austin, Texas 78701.

III. JURISDICTION AND VENUE

30. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 (“CAFA”), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of \$5,000,000 exclusive of interest and costs, there are more than 100 putative class members and minimal diversity exists because Plaintiffs and many putative class members are citizens of a different state than Defendants. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

31. This Court has federal question jurisdiction under 28 U.S.C. § 1331 because this Complaint alleges question of federal laws under the ECPA (18 U.S.C. § 2511, *et seq.*) and VPPA (18 U.S.C. § 2710, *et seq.*).

32. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein from part of the same case or controversy.

33. This Court has personal jurisdiction over Defendants because Defendants have advertised and offered their Website to consumers in the State of California and in this judicial district. Personal jurisdiction is also proper because Defendants committed tortious acts in the State of California and this judicial district and Plaintiffs’ claims arise out of such acts, and/or because Defendants have otherwise made or established contacts

1 in the State of California and in this judicial district sufficient to permit the exercise of
2 personal jurisdiction.

3 34. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(b)
4 because a substantial part of the events giving rise to the claims in this action occurred in
5 this judicial district.

6 **IV. FACTUAL ALLEGATIONS**

7 **A. THE VIDEO PRIVACY PROTECTION ACT**

8 35. The VPPA was passed in 1988 in response to Congress's concern that "the
9 trail of information generated by every transaction that is now recorded and stored in
10 sophisticated record-keeping systems is a new, more subtle and pervasive form of
11 surveillance." S. Rep. No. 100-599, at p. 7 (1988) (statement of Sen. Patrick Leahy).

12 36. In passing the VPPA, Congress was particularly alarmed about surveillance
13 of Americans' media consumption, recognizing that:

14 Books and films are the intellectual vitamins that fuel the growth of
15 individual thought. The whole process of intellectual growth is one of
16 privacy-of quiet, and reflection. This intimate process should be protected
17 from the disruptive intrusion of a roving eye...These records are a window
18 into our loves, lives, and dislikes.

19 *Id.* (statement of Rep. Al McCandless).

20 37. Although the VPPA was originally intended to protect the privacy of an
21 individual's rental videotape selections, Congress has repeatedly reiterated that the VPPA
22 is applicable to "'on-demand' cable services and Internet streaming services [that] allow
23
24
25
26
27

1 consumers to watch movies or TV shows on televisions, laptop computers, and cell
2 phones.” S. Rep. 112-258, at p. 2.⁷

3 38. Under the VPPA, “[a] video tape service provider” is prohibited from
4 “knowingly disclos[ing], to any person, personally identifiable information concerning
5 any consumer of such provider” without the consumer’s “informed, written consent... in
6 a form distinct and separate from any form setting forth other legal or financial obligations
7 of the consumer.” 18 U.S.C. § 2710(b).

8 39. The VPPA defines a “video tape service provider” as “any person, engaged
9 in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery
10 of pre-recorded video cassette tapes or similar audio-visual materials.” 18 U.S.C. §
11 2710(a)(4).

12 40. The VPPA additionally defines “personally identifiable information” as
13 “information which identifies a person as having requested or obtained specific video
14 materials or services from a video service provider.” 18 U.S.C. § 2710(a)(3).

15 41. Defendants are inarguably video tape services provider under the meaning
16 of the VPPA, as its primary business is monetizing access to the millions of pornographic
17 videos hosted on the Website. Accordingly, Defendants’ disclosure of the specific videos
18 viewed by users of the Website, like Plaintiffs’, constitutes a violation of VPPA. *See, e.g.,*
19 *Fan v. NBA Props. Inc.*, No. 23-cv-05069-SI, 2024 U.S. Dist. LEXIS 57205, at *9 (N.D.
20 Cal. Mar. 26, 2024) (“in enacting the VPPA, ‘Congress[] inten[ded] to cover new
21
22

23 ⁷ See also *The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century*, SENATE
24 JUDICIARY, SUBCOMMITTEE ON PRIVACY, TECHNOLOGY AND THE LAW (Jan. 31, 2012), available
25 online at [https://www.judiciary.senate.gov/download/hearing-transcript_-the-video-privacy-
26 protection-act-protecting-viewer-privacy-in-the-21st-century](https://www.judiciary.senate.gov/download/hearing-transcript_-the-video-privacy-protection-act-protecting-viewer-privacy-in-the-21st-century) (statement by Senator Leahy, who
27 originally introduced the VPPA in the Senate: “Now, it is true that technology has changed...but I
28 think we should all agree that we have to be faithful to our fundamental right to privacy and freedom.
Today the social networking, video streaming, the cloud, mobile apps, and other new technologies
have revolutionized the availability of Americans’ information.”).

technologies for pre-recorded video content” and “used ‘similar audio visual materials’ to ensure that VPPA’s protections would retain their force even as technologies evolve”).

B. DEFENDANTS’ USE OF TRACKING TECHNOLOGIES

a. Google’s Mass Advertising Surveillance Operation

42. Google is the largest digital advertiser in the country, accounting for 26.8-percent of the total digital advertising revenue generated in the United States.⁸ In 2023, Google’s advertising revenue of \$238-billion accounted for 77-percent of its total revenue for the year.⁹

43. Google advertises Google Analytics and other Business Tools to website operators, like Defendants, claiming they will allow the operator to “[u]nderstand [their] site and app users,” “check the performance of [their] marketing,” and “[g]et insights only Google can give.”¹⁰ But, in order for website operators to get information from Google Analytics about their website’s visitors, they must allow data collection through installation of Google’s Tracking Tools on their website.¹¹

44. Indeed, on its *Privacy & Terms* page, Google admits that it collects information from third party websites, stating that: “[m]any websites and apps use Google

⁸ *Share of major ad-selling companies in digital advertising revenue in the United States*, STATISTA (May 2024), <https://www.statista.com/statistics/242549/digital-ad-market-share-of-major-ad-selling-companies-in-the-us-by-revenue/#:~:text=In%202023%2C%20Google%20accounted%20for,21.1%20and%2012.5%20percent%2C%20respectively> <https://www.scientificamerican.com/article/7-in-10-smartphone-apps-share-your-data-with-third-party-services/> (last visited Feb. 1, 2025).

⁹ Florian Zandt, *Google's Ad Revenue Dwarfs Competitors*, STATISTA (Sep. 10, 2024), <https://www.statista.com/chart/33017/annual-advertising-revenue-of-selected-tech-companies-offering-search-solutions/#:~:text=Online%20advertising&text=Alphabet%2C%20the%20company%20behind%20the,overall%20revenue%20this%20past%20year> (last visited Feb. 1, 2025).

¹⁰ *Welcome to Google Analytics*, GOOGLE, <https://analytics.google.com/analytics/web/provision/?authuser=0#/provision> (last visited Feb. 1, 2025).

¹¹ See Aaron Ankin & Surya Matta, *The High Privacy Cost of a “Free” Website*, THE MARKUP, <https://themarkup.org/blacklight/2020/09/22/blacklight-tracking-advertisers-digital-privacy-sensitive-websites> (last visited Feb. 1, 2025).

1 services to improve their content and keep it free. When they integrate our services, these
 2 sites and apps share information with Google.”¹²

3 45. Google also admits that it uses the information collected from third party
 4 websites, such as Defendants’, to sell targeted advertising, explaining to users that: “[f]or
 5 example, a website that sells mountain bikes might use Google's ad services. After you
 6 visit that site, you could see an ad for mountain bikes on a different site that shows ads
 7 served by Google.”¹³

8 46. Even though Google admits that it collects information from third-party
 9 websites through the Google Tracking Tools, it does not provide, nor could it provide, a
 10 publicly available list of every webpage on which its Tracking Tools are installed. As
 11 such, the vague descriptions of Google’s data collection practices referenced above could
 12 not give Plaintiffs and Class Members any reason to think that Defendants were part of
 13 Google’s surveillance network.

14 47. Google aggregates the user information that it collects from third-party
 15 websites into ‘advertising profiles’ consisting of all of the data that it has collected about
 16 a given user.¹⁴ With these advertising profiles, Google can sell hyper-precise advertising
 17 services, allowing its clients to target internet users based on combinations of their
 18 location, age, race, interests, hobbies, life events (e.g., recent marriages, graduation, or
 19 relocation), political affiliation, education level, home ownership status, marital status,
 20 household income, type of employment, use of specific apps or websites, and more.¹⁵

21 ¹² *Privacy & Terms – How Google uses information from sites or apps that use our services*, GOOGLE,
 22 <https://policies.google.com/technologies/partner-sites> (last visited Feb. 1, 2025).

23 ¹³ *Id.*

24 ¹⁴ Bennett Cyphers & Gennie Gebhart, *Behind the One-Way Mirror: A Deep Dive Into the Technology*
 25 *of Corporate Surveillance*, ELECTRONIC FRONTIER FOUNDATION (2019), available online at:
https://www EFF.org/files/2019/12/11/behind_the_one-way_mirror-a_deep_dive_into_the_technology_of_corporate_surveillance_0.pdf.

26 ¹⁵ *About audience segments*, GOOGLE ADS, <https://support.google.com/google-ads/answer/2497941?hl=en#zippy=%2Cin-market-segments%2Caffinity-segments%2Clife-events%2Cdetailed-demographics> (last visited Feb. 1, 2025).

48. Google’s surveillance of individual’s internet usage is ubiquitous. In 2017, Scientific American reported that over 70-percent of smartphone apps report “personal data to third-party tracking companies like Google,”¹⁶ and Google trackers are present on 74-percent of all web traffic.

49. Moreover, as in this case, the data collected by Google often pertains to the most personal and sensitive aspects of an individual’s life. For example:

a. 81-percent of the most popular mobile apps for managing depression and quitting smoking allowed Facebook and/or Google to access subscriber information, including health diary entries and self-reports about substance abuse.¹⁷

b. Twelve of the largest pharmacy providers in the United States send information regarding user’s purchases of products such as pregnancy tests, HIV tests, prenatal vitamins, and Plan B to online advertisers.¹⁸ For example, when an online shopper searches for a pregnancy test, views the product page for a pregnancy test, or adds a pregnancy test to their online shopping cart on Kroger’s website, that information is transmitted to Google.¹⁹

¹⁶ Narseo Vallina-Rodriguez & Srikanth Sundaresan, *7 in 10 Smartphone Apps Share Your Data with Third-Party Services*, SCIENTIFIC AMERICAN (May 30, 2017), <https://www.scientificamerican.com/article/7-in-10-smartphone-apps-share-your-data-with-third-party-services/> (last visited Feb. 1, 2025).

¹⁷ Kit Huckvale, John Torous & Mark E. Larsen, *Assessment of the Data Sharing and Privacy Practices of Smartphone Apps for Depression and Smoking Cessation*, JAMA NETWORK OPEN (2019), available online at: <https://pubmed.ncbi.nlm.nih.gov/31002321/>.

¹⁸ Darius Tahir & Simon Fondrie-Teitler, *Need to Get Plan B or an HIV Test Online? Facebook May Know About It*, THE MARKUP (June 30, 2023), <https://themarkup.org/pixel-hunt/2023/06/30/need-to-get-plan-b-or-an-hiv-test-online-facebook-may-know-about-it> (last visited Feb. 1, 2025).

¹⁹ Jon Keegan, *Forget Milk and Eggs: Supermarkets Are Having a Fire Sale on Data About You*, THE MARKUP (Feb. 16, 2023), <https://themarkup.org/privacy/2023/02/16/forget-milk-and-eggs-supermarkets-are-having-a-fire-sale-on-data-about-you> (last visited Feb. 1, 2025).

1
2 50. This monumental, invasive surveillance of Americans' internet usage is not
3 accidental. As Google's then-CEO Eric Schmit admitted in 2010: "We know where you
4 are. We know where you've been. We can more or less know what you're thinking
5 about."²⁰

6 51. In fact, Google values user information so highly that it provides its
7 Business Tools to many website operators for free, all to expand its surveillance
8 apparatus.²¹

9 52. When website operators, like Defendants, make use of Google's Business
10 Tools, they are essentially choosing to participate in Google's mass surveillance network,
11 and in return they benefit from Google's collection of user data, at the expense of their
12 website users' privacy. For example, Google rewards website operators for providing it
13 with their user's information by granting access to its Analytics platform, which leverages
14 demographic data collected by Google to provide detailed analyses of the website's user
15 base.²²

16 **b. Pixels Can Record Almost Every Interaction Between a User and a Website**
17

18 53. In order to use Google's Business Tools, Defendants installed Google's
19 Tracking Tools, including tracking Pixels, onto the Website.

20 54. Pixels are one of the tools used by website operators to track user behavior.
21 As the Federal Trade Commission ("FTC") explains, a Pixel is:

22 [A] small piece of code that will be placed into the website or ad and define
23

24 ²⁰ Andrew Orlowski, *Google's Schmidt: We know what you're thinking*, THE REGISTER (Oct. 4, 2020),
https://www.theregister.com/2010/10/04/google_ericisms/ (last visited Feb. 1, 2025).

25 ²¹ *Analytics Overview*, GOOGLE, <https://marketingplatform.google.com/about/analytics/> (last visited
Feb. 1, 2025) ("Google Analytics gives you the tools, free of charge"),

26 ²² *Google Marketing Platform – Features*, GOOGLE,
<https://marketingplatform.google.com/about/analytics/features/> (last visited Feb. 1, 2025).
27

1 [the Pixel operator's] tracking goals such as purchases, clicks, or
 2 pageviews...

3 Pixel tracking can be monetized several ways. One way to monetize pixel
 4 tracking is for companies to use the tracking data collected to improve the
 5 company's own marketing campaigns...Another is that companies can
 6 monetize the data collected by further optimizing their own ad targeting
 7 systems and charging other companies to use its advertising offerings.²³

8 55. Pixels can collect a shocking amount of information regarding an internet
 9 user's online behavior, including the webpages viewed by the user, the amount of time
 10 spent by the user on specific webpages, the buttons and hyperlinks that the user clicks
 11 while using a website, the items that the user adds to an online shopping cart, the purchases
 12 that a user makes through an online retailer, the text entered by the user into a website
 13 search bar, and even the information provided by the user on an online form.²⁴

14 56. But most internet users are completely unaware that substantial information
 15 about their internet usage is being collected through tracking Pixels. The FTC warns that:
 16 Traditional controls such as blocking third party cookies may not entirely prevent
 17 pixels from collecting and sharing information. Additionally, many
 18 consumers may not realize that tracking pixels exist because they're
 19 invisibly embedded within web pages that users might interact
 20 with...Academic and public reporting teams have found that thousands of
 21 the most visited webpages have pixels and other methods that leak personal

23 ²³ *Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking*, FEDERAL TRADE COMMISSION –
 24 OFFICE OF TECHNOLOGY (Mar. 6, 2023), <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/lurking-beneath-surface-hidden-impacts-pixel-tracking> (last visited Feb. 1, 2025).

25 ²⁴ See *id.*; *How does retargeting on Facebook help your business?*, META,
 26 <https://www.facebook.com/business/goals/retargeting> (last visited Feb. 1, 2025); Tom Kemp, “Oops!
 27 I Did It Again” ... Meta Pixel Still Hoovering Up Our Sensitive Data, MEDIUM,
 28 https://tomkemp00.medium.com/oops-i-did-it-again-meta-pixel-still-hoovering-up-our-sensitive-data-f99c7b779d47#_ftn1 (last visited Feb. 1, 2025).

1 information to third parties.²⁵

2
3 **c. The Pixels Installed on The Website Transmit Personally Identifiable**
4 **Information to Google**

5
6 57. Every website is hosted by a computer “server” that holds the website’s
7 contents.

8 58. To access a website, individuals use “web browsers.” Web browsers are
9 software applications that allow consumers to navigate the web and view and exchange
10 electronic information and communications over the Internet. Each “client device” (such
11 as computer, tablet, or smartphone) accesses web content through a web browser (such as
12 Google’s Chrome, Mozilla’s Firefox, Apple’s Safari, or Microsoft’s Edge).

13 59. Communications between a website server and web browser consist of
14 “Requests” and “Responses.” Any given browsing session may consist of hundreds or
15 even thousands of individual Requests and Responses. A web browser’s Request
16 essentially asks the website to provide certain information, such as the contents of a given
17 webpage when the user clicks a link, and the Response from the website sends back the
18 requested information – the web pages’ images, words, buttons, and other features that
19 the browser shows on the user’s screen as they navigate the website.

20 60. Additionally, on most websites, the Response sent back to the user’s web
21 browser directs the browser to create small files known as ‘cookies’ on the user’s device.²⁶
22 These cookies are saved by the user’s web browser, and are used to identify the website
23 user as they browse the website or on subsequent visits to the site.²⁷ For example, in a

24 _____
25 ²⁵ *Lurking Beneath the Surface*, *supra* note 23.

26 ²⁶ *What is a web browser?*, MOZILLA, <https://www.mozilla.org/en-US/firefox/browsers/what-is-a-browser/> (last visited Feb. 1, 2025).

27 ²⁷ *Id.*

1 more innocuous use case, a cookie may allow the website to remember a user's name and
2 password, language settings, or shopping cart contents.²⁸

3 61. When a Google user logs onto their account, their web browser records a
4 Google tracking cookie.²⁹ This cookie includes a specific line of code that links the web
5 browser to the user's Google account.³⁰

6 62. Google's Pixels use cookies but operate differently than cookies. Rather
7 than directing the browser to save a file on the user's device, the Pixels acquire
8 information from the browser, without notifying the user. The information can include
9 details about the user, his or her interactions with the Website, and information about the
10 user's environment (*e.g.*, type of device, type of browser, and sometimes even the physical
11 location of the device).

12 63. Simultaneously, the Google Pixels, like those installed on The Website,
13 request identifying information from any Google cookies previously installed on the
14 user's web browser.

15 64. The Pixel then combines the data it received from the browser with the data
16 it acquired from the cookie and instructs the web browser to transmit the information back
17 to Google. As a result, Google can link all of the user information collected by their Pixels
18 on the The Website to the user's identity, via the user's Google profile. Thus, even if a
19 user never actually logs into a website or fills out a form, the website, along with Google,
20 can know the user's identity. This is a particularly troubling thought for many people
21 who view pornography from what they think is the privacy of their own home.

22 65. A remarkable number of Americans possess a Google account. Just one of
23 Google's many products, its Gmail e-mail client, is used by over one-third of all
24

25 ²⁸ *Id.*

26 ²⁹ Cyphers, *supra* note 14.

27 ³⁰ *Id.*

1 Americans.³¹ When these internet users visit a website, like Defendants', that utilizes a
2 Google Pixel, any information collected by the Pixel can be linked to the user's identity
3 through the Google cookies installed on the user's web browser.

4 66. However, it is not only Google account holders that are at risk of having
5 Pixel-collected website data linked to their identities. Rather, Google utilizes
6 sophisticated data tracking methods to identify even those few users who do not have a
7 Google account.

8 67. Google's Pixels, like those on The Website, can acquire information about
9 the user's device and browser, such as their screen resolution, time zone setting, browser
10 software type and version, operating system type and version, language setting, and IP
11 address.

12 68. An internet user's combination of such device and browser characteristics,
13 commonly referred to as their "browser fingerprint," is "often unique."³² By tracking this
14 browser fingerprint, Google is able to compile a user's activity across the internet.³³ And,
15 as Google continuously compiles user data over time, its understanding of the user's
16 browser fingerprint becomes more sophisticated such that it needs only to collect a single
17 piece of identifying information to identify the user linked to a browser fingerprint.

18 **d. The TrafficJunky Tracking Tools**

19
20 69. TrafficJunky is an advertising and marketing analytics platform that allows
21 its customers to serve targeted ads on the Pornhub website, as well as other adult websites
22

23
24 ³¹ See Harsha Kiran, *49 Gmail Statistics To Show How Big It Is In 2024*, TECHJURY (Jan. 3, 2024),
25 <https://techjury.net/blog/gmail-statistics/> (last visited Feb. 1, 2025) ("Gmail accounts for 130.9 million
of the total email users in the US"). The United States population is approximately 337.4 million. See
UNITED STATES CENSUS BUREAU, <https://www.census.gov/popclock/> (last visited Feb. 1, 2025).

26 ³² Cyphers, *supra* note 14.

27 ³³ *Id.*

1 operated by the PornHub Defendants.³⁴ By using TrafficJunky, advertisers can set up
 2 advertising campaigns that target Website visitors based on specific criteria, such as
 3 specific region or city, internet service provider, types of device, demographic
 4 information, language, operating system, browser, and even specific keywords search on
 5 the Website.³⁵ TrafficJunky claims to serve 4.63 billion ad impressions *daily*.³⁶

6 70. Shockingly, TrafficJunky allows for and even encourages reprehensible
 7 uses of the Sensitive Information captured from the Website. For example, one reporter
 8 investigating TrafficJunky discovered that it suggested that advertisers target internet
 9 users based on particularly heinous search terms such as “14yrs old,” “tiny girl” and
 10 “screaming teen.”³⁷

11 71. TrafficJunky is able to provide this granular advertising targeting by both
 12 collecting massive amounts of data from Website visitors, correlating that information
 13 with its own cookie identifiers, and then further correlating that data with information
 14 collected from Google’s cookies, as shown in Sec. IV(B)(f), *infra*.

15 **e. Defendants Disclosed Plaintiffs’ and Class Members’ Sensitive Information**
 16 **to Google**

17
 18 72. Unbeknownst to Plaintiffs and Class Members, Pornhub intentionally
 19 configured the Google Pixels installed on the Website to capture and transmit an
 20 enormous amount of the Sensitive Information about them and their use of the Website.

21 73. In their default state as provided by Google, Google’s Pixels record and
 22 transmit only “automatic events,” consisting largely of routine user behavior, such as
 23 clicking a link, clicking on an advertisement, or viewing a webpage. However, the

24 ³⁴ *Networks*, TRAFFICJUNKY, <https://www.trafficjunky.com/online-advertising/networks> (last accessed
 25 Aug. 13, 2025).

26 ³⁵ *Id.*; *Targeting*, TRAFFICJUNKY, <https://www.trafficjunky.com/advertiser/targeting-features> (last
 27 accessed Aug. 13, 2025).

28 ³⁶ *FAQ*, TRAFFICJUNKY, <https://www.trafficjunky.com/resources/faq> (last accessed Aug. 13, 2025).

³⁷ Laila Mickelwait, *Takedown* (Thesis 2024), at p. 241.

1 Google Pixels used on The Website are not in their default state. Instead, Defendants
2 intentionally configured the Pixels on the Website to collect and transmit large amounts
3 of additional user data.

4 74. The below screenshot (“Figure 1”) shows the information requested and
5 transmitted to Google by the Pixels installed on The Website. The information provided
6 in Figure 1 is exemplar information collected on The Website, and is not Plaintiffs’
7 information, but the Pixels installed on The Website collected the same or similar
8 information about Plaintiffs. This includes not just the fact that the user is watching a
9 Pornhub video and the URL of the video, but also the title of the video (in this example it
10 appears next to the cookie labeled “dt:”), the language spoken in the video (next to the
11 cookie labeled “ep.language_spoken_in_video”), the date that the video was uploaded
12 onto Pornhub (next to the cookie labeled “ep.video_date_published”), the sexual
13 orientation associated with the video (e.g., straight, gay, here next to the cookie labeled
14 “ep.video_segment”), whether the video contained formal “pornstars” (next to the cookie
15 labeled “ep.pornstars_in_video”), and the production company that uploaded the video
16 (next to the cookie labeled “ep.video_uploaded_name”).

17 75. All of this information that Defendant transmitted to Google was
18 accompanied by specific lines of code linking the Sensitive Information provided by
19 Plaintiffs and Class Members to their identities. The following screenshot shows that the
20 Google Pixel on The Website transmitted the identifier number attached to Google’s “cid”
21 cookie, which identify the user’s Google account, along with other information that is
22 commonly used to create a browser fingerprint, such as the user’s language preference,
23 screen resolution, browser software and version, operating system software and version,
24 device type (e.g. PC, mobile phone), network type (e.g., cellular, LAN), and internet
25 service provider.

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

```

X Headers Payload Preview Response Initiator Timing Cookies
▼ Query String Parameters view source view URL-encoded
v: 2
tid: G-B39RFFWGY
gtm: 45je54f1v889308053z8892446692za200zb892446692
_p: 1744843151978
gcs: G111
gcd: 13t3t3l3l5l1
npa: 0
dma: 0
tag_exp: 102509683~102803279~102813109~102887800~102926062~103027016~103051953~103055465~103077950~103106314~103106316
cid: 87303652.1744773621
ul: en-us
sr: 1920x1080
uaa: x86
uab: 64
uafvl: Google%20Chrome;135.0.7049.85|Not-A.Brand;8.0.0.0|Chromium;135.0.7049.85
uamb: 0
uam: 0
uap: Windows
uapv: 19.0.0
uaw: 0
are: 1
pae: 1
frm: 0
pscdl: noapi
_eu: AAAAAAI
_s: 1
sid: 1744843099
sct: 4
seg: 1
dl: https://www.pornhub.com/view_video.php?viewkey=67e9cef024d29
dr: https://www.pornhub.com/video
dt: Fuck me while no one's looking - Pornhub.com
en: page_view
ep.active: active
ep.hd video: Yes

```

```

1  ep.language_spoken_in_video: English
2  ep.mpp_geo_blocked: Allowed
3  ep.paid_uvui_video: No
4  ep.pornstars_in_video: No
5  ep.premium_thumbs: Yes
6  ep.premium_video: No
7  ep.up_id: 2565617571
8  ep.video_date_published: 20250330
9  ep.video_duration: 10
10 ep.video_geo_japan: No
11 ep.video_orientation: Straight
12 ep.video_player_version: 8.4.2
13 ep.video_production: Homemade
14 ep.video_reactivated: No
15 ep.video_segment: Straight
16 ep.video_uploader: Amateur Model
17 ep.video_uploader_name: MickLiter
18 ep.dd_related_videos: pornhub.related_video.81
19 ep.dd_recommended_videos: No
20 ep.login_user: No
21 ep.user_interface: pc
22 ep.content_group: videos
23 ep.content_group_2: video
24 ep.referrer_group: video_listing
25 ep.ms_translations: en_none
26 ep.seo_tags_translation: 0
27 ep.watch_page_exp_value: 8
28 up.login_user: No
up.user_interface: pc
up.signup_experiment_value: all
up.orientation: straight
up.shorties_experiment_version: phase_1
up.shorties_exp_2: 8
up.isp: T-Mobile USA
up.connection_type: Cellular
up.seo_tags_translation_user: 0
tfd: 6454

```

Figure 1. Screenshot depicting back-end network traffic from the Website which shows information transmitted to TrafficJunky when Website users watch a video.

76. By installing third-party Tracking Tools, including tracking Pixels, on the Website, and by further custom configuring those Pixels to collect their Website users' Sensitive Information, Defendants knowingly and intentionally caused Plaintiffs' and Class Members' Sensitive Information to be transmitted to third parties, including Google.

f. Pornhub Disclosed Plaintiffs' and Class Members' Sensitive Information to TrafficJunky

77. TrafficJunky's Tracking Tools, internet surveillance tools that are unique to Pornhub's web properties, are also installed on the Website, and also collected Plaintiffs' and Class Members' Sensitive Information.

78. The below screenshot ("Figure 2") shows information requested and transmitted by the Traffic Junky TrafficTools installed on the Website. The information provided in Figure 2 is exemplar information collected on the Website, and is not Plaintiffs' information, but the TrafficJunky Tracking Tools installed on the Website collected the same or similar information about Plaintiffs. This includes not just the fact that the user is watching a Pornhub video and the URL of the video, but also a series of specific tags associated with the video (in this example it appears next to the parameters labeled "channel [context_category]" and "channel [context_tag]"), as well as specific information that is commonly used to create a browser fingerprint, such as the user's device type, screen resolution, browser software and version, and operating system software and version.

79. Importantly, the TrafficJunky Tracking Tools also use Google's cookie identifiers to specifically identify the user. As Figure 2 shows (after the header labeled "cookies"), the TrafficJunky Tracking Tools collect information from Google cookies, including specific identifiers linked to the user's Google account, despite use of Google cookies in this manner constituting a violation of Google's Terms of Service.



Figure 2. Screenshot depicting back-end network traffic from the Website which shows information transmitted to TrafficJunky when Website users watch a video.

80. Additionally, some of the transmissions made by the TrafficJunky Tracking Tools installed on the Website are encoded. With technical know-how, these transmissions can be decoded and reveal even more information harvested by the TrafficJunky Tracking Tools. The below screenshot (“Figure 3”) shows that when decoded, these encoded transmissions include the user’s physical location (in this case, Bellingham, WA).


```

Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
00000000 0A 24 34 38 34 39 33 34 61 62 2D 39 34 38 66 2D .4484934ab-948f-
00000010 34 32 37 64 2D 62 36 36 65 2D 38 38 35 36 61 32 427d-b66e-8856a2
00000020 66 33 33 33 33 33 10 E7 FD C8 C3 06 1A 22 34 62 f33333.cÿEA.."4b
00000030 66 36 65 39 66 35 38 64 38 38 34 31 32 37 62 65 f6e9f58d884127be
00000040 32 63 33 34 37 65 65 63 36 61 33 35 66 31 2D 31 2c347eec6a35f1-1
00000050 28 01 30 05 38 05 48 E0 C4 AF E2 03 52 01 32 58 (.0.8.HaA~a.R.2X
00000060 81 B8 FE DF 03 60 CC B2 CB 86 04 72 20 63 63 61 .,b8.'i+E+.r cca
00000070 37 63 64 39 61 34 62 61 63 34 39 61 30 61 36 65 7cd9a4bac49a0a6e
00000080 64 38 63 35 64 37 35 65 32 62 62 64 38 81 01 8D d8c5d75e2bbd8...
00000090 ED B5 A0 F7 C6 00 3F 92 01 02 55 53 9A 01 02 57 ip +E.?'..US$.W
000000A0 41 A2 01 0A 42 65 6C 6C 69 6E 67 68 61 6D AA 01 Ac..Bellingham".
000000B0 B5 01 61 73 69 61 6E 20 64 65 65 70 74 68 72 6F u.asian deepthro
000000C0 61 74 2C 62 65 73 74 20 64 6F 67 67 79 73 74 79 at,best doggysty
000000D0 6C 65 2C 62 69 67 20 61 73 73 2C 62 69 67 20 61 le,big ass,big a
000000E0 73 73 2C 62 69 67 20 64 69 63 6B 2C 62 6C 6F 77 ss,big dick,blow
000000F0 6A 6F 62 2C 62 6C 6F 77 6A 6F 62 2C 62 6C 6F 77 job,blowjob,blow
00000100 6A 6F 62 20 63 75 6D 20 69 6E 20 6D 6F 75 74 68 job cum in mouth
00000110 2C 62 6C 6F 77 6A 6F 62 20 70 6F 76 2C 62 72 75 ,blowjob pov,bru
00000120 6E 65 74 74 65 2C 63 75 6D 73 68 6F 74 2C 68 64 nette,cumshot,hd
00000130 20 70 6F 72 6E 2C 70 6F 76 2C 72 6F 75 67 68 20 porn,pov,rough
00000140 73 65 78 2C 72 75 73 73 69 61 6E 2C 73 69 64 65 sex,russian,side
00000150 20 66 75 63 6B 2C 76 65 72 69 66 69 65 64 20 61 fuck,verified a
00000160 6D 61 74 65 75 72 73 CA 01 0D 63 6F 6D 63 61 73 mateurs$.comcas
00000170 74 20 63 61 62 6C 65 D2 01 04 77 69 66 69 DA 01 t cable0..wifi0.
00000180 07 77 69 6E 64 6F 77 73 E2 01 0C 37 33 2E 32 32 .windows$.73.22
00000190 35 2E 34 33 2E 35 36 FA 01 0C 37 33 2E 32 32 35 5.43.56$.73.225
000001A0 2E 34 33 2E 35 36 82 02 07 64 65 64 33 33 34 35 .43.56,...ded3345
000001B0 92 02 04 65 64 67 65 9A 02 05 39 38 32 32 35 AA '..edges$.98225*
000001C0 02 04 31 31 2E 30 B2 02 03 31 33 38 D8 02 B0 83 ..11.0*...1380.*f
000001D0 95 F5 07 E0 02 DC EC CA B0 04 F2 02 24 39 36 32 *.â.ÜiÊ*.ô.$962
000001E0 32 33 39 66 33 2D 64 62 35 61 2D 61 30 39 37 2D 239f3-db5a-a097-
000001F0 30 61 37 33 2D 34 31 39 38 64 36 30 33 30 39 35 0a73-4198d603095
00000200 35 FA 02 01 31 82 03 8F 01 7B 22 61 63 74 6F 72 5û..l,...{"actor
00000210 5F 69 64 22 3A 32 35 36 35 36 31 37 35 37 31 2C _id":2565617571,
00000220 22 63 6F 6E 74 65 6E 74 5F 74 79 70 65 22 3A 22 "content_type":
00000230 6D 6F 64 65 6C 22 2C 22 76 69 64 65 6F 5F 69 64 model","video_id
00000240 22 3A 34 36 39 34 38 32 31 32 35 2C 22 68 61 73 ":469482125,"has
00000250 68 22 3A 22 32 32 63 61 33 63 38 66 62 61 32 34 h":"22ca3c8fba24
00000260 36 35 62 62 63 30 63 62 63 31 39 65 35 30 34 37 65bbc0cbc19e5047
00000270 34 66 30 32 22 2C 22 73 65 73 73 69 6F 6E 5F 69 4f02","session_i
00000280 64 22 3A 22 33 39 38 33 36 32 31 38 39 35 30 32 d":"398362189502
00000290 38 39 31 32 34 30 22 7D 92 03 07 64 65 73 6B 74 891240")'..deskt
000002A0 6F 70 9A 03 02 65 6E C2 03 05 76 69 64 65 6F D2 op$.enâ..video0
000002B0 04 06 AF 05 BD 05 F1 07 E8 04 DC FC FF FF FF FF ..$.â.â.Uuyyyy
000002C0 FF FF FF 01 yyy.

```

Figure 3. Screenshot depicting back-end network traffic from the Website which shows information transmitted to TrafficJunky when Website users watch a video.

C. DEFENDANTS DISCLOSED PLAINTIFFS' AND CLASS MEMBERS' SENSITIVE INFORMATION TO THIRD PARTIES WITHOUT THEIR KNOWLEDGE OR CONSENT

a. The Tracking Tools Used by Defendants Were Imperceptible to Plaintiffs and Class Members

81. The Tracking Tools installed on the Website were invisible to Plaintiffs and Class Members. Without analyzing the network information transmitted by the Website

1 through examination of its source code or the use of sophisticated web developer tools,
2 there was no way for a Website user to discover the presence of the Tracking Tools. As a
3 result, typical internet users, such as Plaintiffs and Class Members, were unable to detect
4 the Tracking Tools on the Website.

5 82. Plaintiffs and Class Members were shown no disclaimer or warning that
6 their Sensitive Information would be disclosed to any unauthorized third party without
7 their express consent.

8 83. Plaintiffs and Class Members did not know that their Sensitive Information
9 was being collected and transmitted to an unauthorized third party.

10 84. Because Plaintiffs and Class Members were not aware of the Tracking Tools
11 on the website, or that their Sensitive Information would be collected and transmitted to
12 Google, they could not and did not consent to Defendants' conduct.

13 **D. DEFENDANTS WERE ENRICHED BY ITS DISCLOSURE OF**
14 **PLAINTIFFS' AND CLASS MEMBERS' SENSITIVE INFORMATION**
15 **TO THIRD PARTIES**

16 **a. Defendants Received Material Benefits in Exchange for Plaintiffs' Sensitive**
17 **Information**

18
19 85. As explained, *supra*, users of Google's Business Tools, like Pornhub,
20 receive access to advertising and marketing analytics services in exchange for installing
21 Google's Tracking Tools on their website.

22 86. Upon information and belief, Pornhub, as users of Google's Business Tools,
23 received compensation in the form of advanced advertising services and cost-effective
24 marketing on third-party platforms in exchange for allowing Google to collect Plaintiffs'
25 and Class Members' Sensitive Information.

b. Plaintiffs' and Class Members' Data Had Financial Value

87. Moreover, Plaintiffs' and Class Members' Sensitive Information had value, and Defendants' disclosure and interception of that Sensitive Information harmed Plaintiffs and the Class.

88. According to the financial statements of Facebook, another major seller of online advertisements, the value derived from user data has continuously risen. "In 2013, the average American's data was worth about \$19 per year in advertising sales to Facebook, according to its financial statements. In 2020, [it] was worth \$164 per year."³⁸

89. Conservative estimates suggest that in 2018, Internet companies earned \$202 per American user from mining and selling data. That figure is only due to keep increasing; estimates for 2022 are as high as \$434 per user, for a total of more than \$200 billion industry wide.

90. Several companies have products through which they pay consumers for a license to track certain information. Google, Nielsen, UpVoice, HoneyGain, and SavvyConnect are all companies that pay for browsing history information.

91. The unauthorized disclosure of Plaintiffs' and Class Members' private and Sensitive Information has diminished the value of that information, resulting in harm to Plaintiffs and Class Members.

E. PLAINTIFFS' AND CLASS MEMBERS' REASONABLE EXPECTATION OF PRIVACY

92. At all times when Plaintiffs and Class Members provided their Sensitive Information to Pornhub, they each had a reasonable expectation that the information

³⁸ Geoffrey A. Fowler, *There's no escape from Facebook, even if you don't use it*, THE WASHINGTON POST (Aug. 29, 2021), <https://www.washingtonpost.com/technology/2021/08/29/facebook-privacy-monopoly/> (last visited Feb. 1, 2025).

1 would remain confidential and that Pornhub would not share the Sensitive Information
 2 with third parties for a commercial purpose, unrelated to processing their loan
 3 applications.

4 93. Privacy polls and studies show that the overwhelming majority of
 5 Americans consider obtaining an individual's affirmative informed consent before a
 6 company collects and shares that individual's data to be one of the most important privacy
 7 rights.

8 94. For example, a recent Consumer Reports study shows that 92-percent of
 9 Americans believe that internet companies and websites should be required to obtain
 10 consent before selling or sharing consumer data, and the same percentage believe those
 11 companies and websites should be required to provide consumers with a complete list of
 12 the data that is collected about them.³⁹

13 95. Individuals are particularly sensitive about disclosure of information
 14 relating to pornography usage. Extensive research has shown that pornography usage is
 15 nearly ubiquitously linked to significant feelings of shame, particularly because of the
 16 societal stigma attached to the consumption of pornography.⁴⁰ As a result, qualitative

17
 18 ³⁹ *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*,
 19 CONSUMER REPORTS (May 11, 2017), <https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety-a3980496907> (last
 visited Feb. 1, 2025).

20 ⁴⁰ See Wendy G. Macdowall, *et al.*, *Pornography Use Among Adults in Britain: A Qualitative Study of*
 21 *Patterns of Use, Motivations, and Stigma Management Strategies*, ARCH. SEX. BEHAV. (Apr. 3, 2025),
 at p. 2, available online at: <https://link.springer.com/article/10.1007/s10508-025-03112-7> (compiling
 22 studies finding shame and social stigma associated with pornography); Luke Sniewski and Pani
 23 Farvid, *Hidden in Shame: Heterosexual Men's Experiences of Self-Perceived Problematic*
Pornography Use, 21(2) PSYCH. MEN & MASC. 210 (July 18, 2019), available online at:
 24 <https://www.lukesniewski.com/wp-content/uploads/2019/09/Hidden-in-Shame.pdf> ("The main reason
 25 men kept their viewing hidden from the world was because of the accompanying experiences of guilt
 26 and shame that would inevitably follow most—if not all—viewing sessions"); Michael Tholander,
 Sofia Johansson, Klara Thunell and Örjan Dahlström, *Traces of Pornography: Shame, Scripted Action,*
 27 *and Agency in Narratives of Young Swedish Women*, 26 SEXUAL. & CULT. 1826 (May 11, 2022)
 (noting "private and silent shame" associated with pornography consumption due to attitudes that
 28 viewing pornography is "'dirty,' 'disgusting,' 'hideous,' 'repugnant,' 'unnatural,' and 'vulgar'"),
 available online at: <https://link.springer.com/article/10.1007/s12119-022-09973-7/>.

1 studies have showed that the most common behavior among those who consume
2 pornography is “keeping their pornography viewing secret from others, such as partners
3 and family.”⁴¹

4 96. Personal data privacy and obtaining consent to share Sensitive Information
5 are material to Plaintiffs and Class Members.

6 **V. TOLLING AND ESTOPPEL**

7
8 97. Any applicable statutes of limitation have been tolled by Defendants’
9 knowing and active concealment of its incorporation of the Tracking Tools into the
10 Website.

11 98. The Pixels and other tracking tools on the Website were and are invisible to
12 the average website visitor.

13 99. Through no fault or lack of diligence, Plaintiffs and Class Members were
14 deceived and could not reasonably discover Defendants’ deception and unlawful conduct.

15 100. Plaintiffs were ignorant of the information essential to pursue their claims,
16 without any fault or lack of diligence on their part.

17 101. Defendants had exclusive knowledge that the Website incorporated the
18 Tracking Tools and yet failed to disclose to Website users, including Plaintiffs and Class
19 Members, that by visiting the Website, Plaintiffs’ and Class Members’ Sensitive
20 Information would be disclosed or released to unauthorized third parties, including
21 Google and TrafficJunky.

22 102. Under the circumstances, Defendants were under a duty to disclose the
23 nature, significance, and consequences of their collection and treatment of Website users’
24 Sensitive Information. In fact, Defendants still have not conceded, acknowledged, or
25 otherwise indicated to their customers that they have disclosed or released their Sensitive

26 _____
27 ⁴¹ Macdowall, *supra* note 32, at pp. 3-8.

1 Information to unauthorized third parties. Accordingly, Defendants are estopped from
2 relying on any statute of limitations.

3 103. Moreover, all applicable statutes of limitation have also been tolled
4 pursuant to the discovery rule.

5 104. The earliest that Plaintiffs or Class Members, acting with due diligence,
6 could have reasonably discovered Defendants' conduct would have been shortly before
7 the filing of this Complaint.

8 **VI. CLASS ALLEGATIONS**

9
10 105. This action is brought by the named Plaintiffs both individually, and on
11 behalf of a proposed Class of all other persons similarly situated under Federal Rules of
12 Civil Procedure 23(b)(2), 23(b)(3), and 23(c)(4).

13 106. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

14 **The Nationwide Class**

15
16 All natural persons who watched a video on the Website, and whose Sensitive
17 Information was disclosed or transmitted Google, TrafficJunky or any other
18 unauthorized third party.

19
20 107. In addition to the claims asserted on behalf of the Nationwide Class,
21 Plaintiffs assert claims on behalf of separate California and New York Subclasses, which
22 are defined as follows:

23 **California Subclass**

24
25 All natural persons residing in California who watched a video on the Website, and
26 whose Sensitive Information was disclosed or transmitted Google, TrafficJunky or

1 any other unauthorized third party.

2
3 **New York Subclass**
4

5 All natural persons residing in New York who watched a video on the Website, and
6 whose Sensitive Information was disclosed or transmitted Google, TrafficJunky or
7 any other unauthorized third party.
8

9 108. Excluded from the proposed Class are any claims for personal injury,
10 wrongful death, or other property damage sustained by the Class; and any Judge
11 conducting any proceeding in this action and members of their immediate families.

12 109. Plaintiffs reserve the right to amend the definitions of the Class or add
13 subclasses if further information and discovery indicate that the definitions of the Class
14 should be narrowed, expanded, or otherwise modified.

15 110. **Numerosity.** The Class is so numerous that the individual joinder of all
16 members is impracticable. There are at least 10,000 individuals that have been impacted
17 by Defendants' actions. Moreover, the exact number of those impacted is generally
18 ascertainable by appropriate discovery and is in the exclusive control of Defendants.

19 111. **Commonality.** Common questions of law or fact arising from Defendants'
20 conduct exist as to all members of the Class, which predominate over any questions
21 affecting only individual Class Members. These common questions include, but are not
22 limited to, the following:

- 23 a) Whether and to what extent Defendants had a duty to protect
24 the Sensitive Information of Plaintiffs and Class Members;
25
26
27

- 1 b) Whether Defendants had duties not to intercept and/or disclose
2 the Sensitive Information of Plaintiffs and Class Members to
3 unauthorized third parties;
4
- 5 c) Whether Defendants adequately, promptly, and accurately
6 informed Plaintiffs and Class Members that their Sensitive
7 Information would be disclosed to third parties;
8
- 9 d) Whether Defendants violated the law by failing to promptly
10 notify Plaintiffs and Class Members that their Sensitive
11 Information was being disclosed without their consent;
12
- 13 e) Whether Defendants adequately addressed and fixed the
14 practices which permitted the unauthorized disclosure of
15 patients' Sensitive Information;
16
- 17 f) Whether Defendants engaged in unfair, unlawful, or deceptive
18 practices by failing to keep the Sensitive Information belonging
19 to Plaintiffs and Class Members free from unauthorized
20 disclosure;
21
- 22 g) Whether Defendants violated the Video Privacy Protection Act,
23 as alleged in this Complaint;
24
25
26
27

1 h) Whether Plaintiffs and Class Members are entitled to actual,
2 consequential, and/or nominal damages as a result of
3 Defendants' wrongful conduct;

4
5 i) Whether Plaintiffs and Class Members are entitled to injunctive
6 relief to redress the imminent and currently ongoing harm faced
7 as a result of the Defendants' disclosure of their Sensitive
8 Information.

9
10 112. **Typicality**. Plaintiffs' claims are typical of those of other Class Members
11 because Plaintiffs' Sensitive Information, like that of every other Class Member, was
12 compromised as a result of Defendants' incorporation and use of the Tracking Tools.

13 113. **Adequacy**. Plaintiffs will fairly and adequately represent and protect the
14 interests of the members of the Class in that Plaintiffs have no disabling conflicts of
15 interest that would be antagonistic to those of the other members of the Class. Plaintiffs
16 seek no relief that is antagonistic or adverse to the members of the Class and the
17 infringement of the rights and the damages Plaintiffs have suffered are typical of other
18 Class Members. Plaintiffs have also retained counsel experienced in complex class action
19 litigation, and Plaintiffs intend to prosecute this action vigorously.

20 114. **Predominance**. Defendants have engaged in a common course of conduct
21 toward Plaintiffs and Class Members in that all the Plaintiffs' and Class Members' data
22 was unlawfully intercepted, stored and disclosed to unauthorized third parties, including
23 third parties, like Google and TrafficJunky, in the same way. The common issues arising
24 from Defendants' conduct affecting Class Members set out above predominate over any
25 individualized issues. Adjudication of these common issues in a single action has
26 important and desirable advantages of judicial economy.

1 115. **Superiority.** A class action is superior to other available methods for the
2 fair and efficient adjudication of the controversy. Class treatment of common questions
3 of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a
4 class action, most Class Members would likely find that the cost of litigating their
5 individual claim is prohibitively high and would therefore have no effective remedy. The
6 prosecution of separate actions by individual Class Members would create a risk of
7 inconsistent or varying adjudications with respect to individual Class Members, which
8 would establish incompatible standards of conduct for Defendants. In contrast, the
9 conduct of this action as a class action presents far fewer management difficulties,
10 conserves judicial resources and the parties' resources, and protects the rights of each
11 Class Member.

12 116. Defendants acted on grounds that apply generally to the Class as a whole so
13 that class certification, injunctive relief, and corresponding declaratory relief are
14 appropriate on a class-wide basis.

15 117. Likewise, particular issues under Fed. R. Civ. P. 23(c)(4) are appropriate
16 for certification because such claims present only particular, common issues, the
17 resolution of which would advance the disposition of this matter and the parties' interests
18 therein. Such particular issues include, but are not limited to:

19 a) Whether Defendants owed a legal duty to Plaintiffs and the Class
20 to exercise due care in collecting, storing, and safeguarding their
21 Sensitive Information and/or not disclosing it to unauthorized
22 third parties;

23
24 b) Whether Defendants breached a legal duty to Plaintiffs and
25 Class Members to exercise due care in collecting, storing, using,
26 and safeguarding their Sensitive Information;

- 1
- 2 c) Whether Defendants failed to comply with applicable laws,
- 3 regulations, and industry standards relating to data security;
- 4
- 5 d) Whether Defendants adequately and accurately informed
- 6 Plaintiffs and Class Members that their Sensitive Information
- 7 would be disclosed to third parties;
- 8
- 9 e) Whether Defendants failed to implement and maintain
- 10 reasonable security procedures and practices appropriate to the
- 11 nature and scope of the information disclosed to third parties;
- 12
- 13 f) Whether Class Members are entitled to actual, consequential,
- 14 and/or nominal damages and/or injunctive relief as a result of
- 15 Defendants' wrongful conduct.

16 118. Finally, all members of the proposed Class are readily ascertainable.

17 Defendants have access to Class Members' names and addresses affected by the

18 unauthorized disclosures that have taken place.

19

20 **COUNT I**

21 **COMMON LAW INVASION OF PRIVACY**

22 **(On Behalf of Plaintiffs and the Nationwide Class or, alternatively, the California**

23 **and New York Subclasses)**

24 119. Plaintiffs repeat and reallege the allegations contained in paragraphs 1

25 through 118 as if fully set forth herein.

26 120. Plaintiffs and Class Members have an interest in: (1) precluding the

27 dissemination and/or misuse of their sensitive, highly personal Sensitive Information; and

28 (2) making personal decisions and/or conducting personal activities without observation,

1 intrusion or interference, including, but not limited to, the right to visit and interact with
2 various internet sites without being subjected to the exfiltration of their communications
3 without Plaintiffs' and Class Members' knowledge or consent.

4 121. Plaintiffs and Class Members had a reasonable expectation of privacy in
5 their communications with Defendants via the Website and the communications platforms
6 and services therein.

7 122. Plaintiffs and Class Members communicated Sensitive Information that
8 they intended for only Defendants to receive and that they understood Defendants would
9 keep private and secure.

10 123. Defendants' interception and disclosure of the substance and nature of those
11 communications to third parties without the knowledge and informed consent of Plaintiffs
12 and Class Members is an intentional intrusion on Plaintiffs' and Class Members' solitude
13 or seclusion.

14 124. Plaintiffs and Class Members have a general expectation that their
15 communications regarding sensitive, highly personal information would be protected
16 from surreptitious disclosure to third parties.

17 125. Defendants' disclosure and publicization of Plaintiffs' and Class Members'
18 Sensitive Information coupled with individually identifying information is highly
19 offensive to the reasonable person.

20 126. As a result of Defendants' actions, Plaintiffs and Class Members have
21 suffered harm and injury including, but not limited to, an invasion of their privacy rights.

22 127. Plaintiffs and Class Members have been damaged as a direct and proximate
23 result of Defendants' invasion of their privacy and are entitled to compensatory and/or
24 nominal damages.

25 128. Plaintiffs and Class Members seek appropriate relief for that injury
26 including, but not limited to, damages that will reasonably compensate Plaintiffs and

1 Class Members for the harm to their privacy interests as a result of the intrusions upon
2 their privacy.

3 129. Plaintiffs and Class Members are also entitled to punitive damages resulting
4 from the malicious, willful and intentional nature of Defendants' actions, directed at
5 injuring Plaintiffs and Class Members in conscious disregard of their rights. Such
6 damages are needed to deter Defendants from engaging in such conduct in the future.

7 130. Plaintiffs also seek such other relief as the Court may deem just and proper.

8
9 **COUNT II**
10 **NEGLIGENCE**
(On Behalf of Plaintiffs and the Nationwide Class or, alternatively, the California
and New York Subclasses)

11 131. Plaintiffs repeat and reallege the allegations contained in paragraphs 1
12 through 130 as if fully set forth herein.

13 132. Through using The Website, Plaintiffs and Class Members provided them
14 with their Sensitive Information.

15 133. By collecting and storing data related to Plaintiffs and Class Members use
16 of the Website, Defendants had a duty of care to use reasonable means to secure and
17 safeguard it from unauthorized disclosure to third parties.

18 134. Defendants negligently, recklessly, and/or intentionally failed to take
19 reasonable steps to protect Plaintiffs' and Class Members' Sensitive Information from
20 being disclosed to third parties, without their consent, including to Google.

21 135. Defendants further negligently, recklessly, and/or intentionally omitted to
22 inform Plaintiffs and the Class that it would use their Sensitive Information for marketing
23 purposes, or that their Sensitive Information would be transmitted to third parties.

24 136. Defendants knew, or reasonably should have known, that Plaintiffs and the
25 Class would not have provided their Sensitive Information to Defendants, had Plaintiffs
26 and the Class known that Defendants intended to use that information for unlawful

1 purposes.

2 137. Defendants' conduct has caused Plaintiffs and the Class to suffer damages
3 by having their highly confidential, personally identifiable Sensitive Information
4 accessed, stored, and disseminated without their knowledge or consent.

5 138. Plaintiffs and Class Members are entitled to compensatory, nominal, and/or
6 punitive damages.

7 139. Defendants' negligent conduct is ongoing, in that they still hold the
8 Sensitive Information of Plaintiffs and Class Members in an unsafe and unsecure manner.
9 Therefore, Plaintiffs and Class Members are also entitled to injunctive relief requiring
10 Defendants to (i) strengthen their data security systems and monitoring procedures; (ii)
11 cease collection and dissemination of the Website users' Sensitive Information to third
12 parties; and (iii) submit to future annual audits of those systems and monitoring
13 procedures.

14 **COUNT III**
15 **BREACH OF IMPLIED CONTRACT**
16 **(On Behalf of Plaintiffs and the Nationwide Class or, alternatively, the California**
17 **and New York Subclasses)**

18 140. Plaintiffs repeat and reallege the allegations contained in paragraphs 1
19 through 139 as if fully set forth herein.

20 141. When Plaintiffs and Class Members provided their Sensitive Information to
21 Defendants in exchange for services, they entered into an implied contract pursuant to
22 which Defendants agreed to safeguard and not disclose their Sensitive Information
23 without consent.

24 142. Plaintiffs and Class Members accepted Defendants' offers and provided
25 their Sensitive Information to Defendants.

26 143. Plaintiffs and Class Members would not have entrusted Defendants with
27 their Sensitive Information in the absence of an implied contract between them and
28 Defendants obligating Defendants to not disclose Sensitive Information without consent.

1 144. Defendants breached these implied contracts by disclosing Plaintiffs' and
2 Class Members' Sensitive Information to third parties like Google and TrafficJunky .

3 145. As a direct and proximate result of Defendants' breaches of these implied
4 contracts, Plaintiffs and Class Members sustained damages as alleged herein.

5 146. Plaintiffs and Class Members would not have used Defendants' services had
6 they known their Sensitive Information would be disclosed.

7 147. Plaintiffs and Class Members are entitled to compensatory, consequential,
8 and/or nominal damages as a result of Defendants' breaches of implied contract.

9
10 **COUNT IV**
11 **UNJUST ENRICHMENT**
12 **(On Behalf of Plaintiffs and the Nationwide Class or, alternatively, the California**
13 **and New York Subclasses)**

14 148. Plaintiffs repeat and reallege the allegations contained in paragraphs 1
15 through 147 as if fully set forth herein.

16 149. Plaintiffs plead this claim in the alternative to their breach of implied
17 contract claim.

18 150. Plaintiffs and Class Members conferred a monetary benefit on Defendants.
19 Specifically, they provided their Sensitive Information to Defendants, which Defendants
20 exchanged for marketing and advertising services, as described, *supra*.

21 151. Defendants knew that Plaintiffs and Class Members conferred a benefit
22 which Defendants accepted. Defendants profited from the Sensitive Information of
23 Plaintiffs and Class Members by exchanging it for marketing and advertising services.

24 152. In particular, Defendants enriched themselves by obtaining the inherent
25 value of Plaintiffs' and Class Members' Sensitive Information, and by exchanging
26 Plaintiffs' and Class Members' Sensitive Information to third parties, like Google, in
27 exchange for advertising and marketing services.

28 153. Plaintiffs and Class Members, on the other hand, suffered as a direct and

1 proximate result of Defendants' decision to prioritize their own profits over the privacy
2 of their Sensitive Information.

3 154. Under the principles of equity and good conscience, Defendants should not
4 be permitted to retain the money belonging to Plaintiffs and Class Members, obtained by
5 its surreptitious collection and transmission of their Sensitive Information.

6 155. If Plaintiffs and Class Members knew that Defendants had not reasonably
7 secured their Sensitive Information, they would not have agreed to provide their Sensitive
8 Information to Defendants.

9 156. Plaintiffs and Class Members have no adequate remedy at law for this count.
10 An unjust enrichment theory provides the equitable disgorgement of profits even where
11 an individual has not suffered a corresponding loss in the form of money damage.

12 157. As a direct and proximate result of Defendants' conduct, Plaintiffs and
13 Class Members have suffered and will continue to suffer injury.

14 158. Defendants should be compelled to disgorge into a common fund or
15 constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they
16 unjustly received from them, or to refund the amounts that Plaintiffs and Class Members
17 overpaid for Defendants' services.

18
19 **COUNT V**
20 **VIOLATIONS OF THE VIDEO PRIVACY PROTECTION ACT**
21 **18 U.S.C. § 2710, et seq.**
22 **(On Behalf of Plaintiffs and the Nationwide Class or, alternatively, the California**
23 **Subclass)**

24 159. Plaintiffs repeat and reallege the allegations contained in paragraphs 139
25 through 149 as if fully set forth herein.

26 160. The VPPA provides that "a video tape service provider who knowingly
27 discloses, to any person, personally identifiable information concerning any consumer
28 shall be liable to the aggrieved person[.]" 18 U.S.C. § 2710(b)(1).

1 161. “Personally-identifiable information” is defined to include “information
2 which identifies a person as having requested or obtained specific video materials or
3 services from a video tape service provider.” 18 U.S.C. § 2710(a)(3).

4 162. A “video tape service provider” is “any person, engaged in the business, in
5 or affecting interstate commerce, of rental, sale, or delivery of pre-recorded video cassette
6 tapes or similar audio visual materials.” 18 U.S.C. § 2710(a)(4).

7 163. Defendants are both a “video tape service provider” because their primary
8 business is the production, hosting, and streaming of millions of videos on the Website,
9 thereby “engag[ing] in the business, in or affecting interstate or foreign commerce, of
10 rental, sale, or delivery of pre-recorded video cassette tapes or similar audio visual
11 materials.” 18 U.S.C. § 2710(a)(4).

12 164. Defendants violated the VPPA by knowingly disclosing Plaintiffs’ and
13 Class Members’ personally identifiable information to Google through the Tracking Tools
14 without obtaining informed, written consent.

15 165. As a result of Defendants’ violations of the VPPA, Plaintiffs and the Class
16 are entitled to all damages available under the VPPA including declaratory relief,
17 injunctive and equitable relief, statutory damages of \$2,500 for each violation of the
18 VPPA, and attorney’s fees, filing fees, and costs.

19
20 **COUNT VI**
21 **VIOLATIONS OF THE ELECTRONIC COMMUNICATIONS PRIVACY**
22 **ACT (“ECPA”), 18 U.S.C. § 2511(1), et seq.**
23 **Unauthorized Interception, Use, and Disclosure**
24 **(On Behalf of Plaintiffs and the Nationwide Class or, alternatively, the California**
25 **and New York Subclasses)**

26 166. Plaintiffs repeat and reallege the allegations contained in paragraphs 1
27 through 165 as if fully set forth herein.

28 167. The ECPA protects both sending and receipt of communications.

169. The transmissions of Plaintiffs' Sensitive Information to The Website qualify as "communications" under the ECPA's definition of 18 U.S.C. § 2510(12).

170. Electronic Communications. The transmission of Sensitive Information between Plaintiffs and Class Members and The Website with which they chose to exchange communications are “transfer[s] of signs, signals, writing,...data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce” and are therefore “electronic communications” within the meaning of 18 U.S.C. § 2510(2).

13 171. Content. The ECPA defines content, when used with respect to electronic
14 communications, to “include[] any information concerning the substance, purport, or
15 meaning of that communication.” 18 U.S.C. § 2510(8) (emphasis added).

16 172. Interception. The ECPA defines the interception as the “acquisition of the
17 contents of any wire, electronic, or oral communication through the use of any electronic,
18 mechanical, or other device” and “contents ... include any information concerning the
19 substance, purport, or meaning of that communication.” 18 U.S.C. § 2510(4), (8).

173. Electronic, Mechanical or Other Device. The ECPA defines “electronic,
mechanical, or other device” as “any device ... which can be used to intercept a[n] ...
electronic communication[.]” 18 U.S.C. § 2510(5). The following constitute “devices”
within the meaning of 18 U.S.C. § 2510(5):

- 24 a. Plaintiffs' and Class Members' browsers;
- 25 b. Plaintiffs' and Class Members' computing devices;
- 26 c. Defendants' web-servers; and

1 d. The Pixel code deployed by Defendants to effectuate the sending
2 and acquisition of patient communications.

3 174. By utilizing and embedding the Pixels on the Website, Defendants
4 intentionally intercepted, endeavored to intercept, and procured another person to
5 intercept, the electronic communications of Plaintiffs and Class Members, in violation of
6 18 U.S.C. § 2511(1)(a).

7 175. Specifically, Defendants intercepted Plaintiffs' and Class Members'
8 electronic communications via the Pixels, which tracked, stored, and unlawfully disclosed
9 Plaintiffs' and Class Members' Sensitive Information to third parties such as Google.

10 176. Defendants' intercepted communications include, but are not limited to,
11 communications to/from Plaintiffs and Class Members regarding their Sensitive
12 Information, including their applications for a debt consolidation loan, and the
13 determination of whether or not to grant those loans.

14 177. By intentionally disclosing or endeavoring to disclose the electronic
15 communications of Plaintiffs and Class Members to third parties, while knowing or
16 having reason to know that the information was obtained through the interception of an
17 electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendants violated 18
18 U.S.C. § 2511(1)(c).

19 178. By intentionally using, or endeavoring to use, the contents of the electronic
20 communications of Plaintiffs and Class Members, while knowing or having reason to
21 know that the information was obtained through the interception of an electronic
22 communication in violation of 18 U.S.C. § 2511(1)(a), Defendants violated 18 U.S.C. §
23 2511(1)(d).

24 179. Unauthorized Purpose. Defendants intentionally intercepted the contents of
25 Plaintiffs' and Class Members' electronic communications for the purpose of committing
26

1 a tortious act in violation of the Constitution or laws of the United States or of any State—
2 namely, invasion of privacy, among others.

3 180. The ECPA provides that a “party to the communication” may liable where
4 a “communication is intercepted for the purpose of committing any criminal or tortious
5 act in violation of the Constitution or laws of the United States or of any State.” 18 U.S.C
6 § 2511(2)(d).

7 181. Pornhub is not a party for purposes to the communication based on its
8 unauthorized duplication and transmission of communications with Plaintiffs and the
9 Class. However, even assuming Pornhub is a party, Pornhub’s simultaneous, unknown
10 duplication, forwarding, and interception of Plaintiffs’ and Class Members’ Sensitive
11 Information does not qualify for the party exemption.

12 182. Defendants’ acquisition of sensitive communications that were used and
13 disclosed to Google and TrafficJunky was done for purposes of committing criminal and
14 tortious acts in violation of the laws of the United States and individual States nationwide
15 as set forth herein, including:

- 16 a. Invasion of privacy;
- 17 b. Breach of confidence;
- 18 c. Breach of implied contract;
- 19 d. Violations of the Video Privacy Protection Act, 18 U.S.C. § 2710, *et seq.*;
- 20 e. Violations of N.Y. Gen. Bus. Law § 349;
- 21 f. Violations of the California Invasion of Privacy Act, Cal. Pen. Code § 360,
22 *et seq.*; and
- 23 g. Violations of the California Unfair Competition Law, Cal. Bus. & Prof.
24 Code, § 17200, *et seq.*

25 183. Defendants’ conduct violated 42 U.S.C. § 1320d-6 in that it used and caused
26 to be used cookie identifiers associated with specific users, including Plaintiffs and Class

Members, without user authorization; and disclosed individually identifiable Sensitive Information to Google and TrafficJunky without user authorization.

184. Defendants are not exempt from ECPA liability under 18 U.S.C. § 2511(2)(d) on the ground that it was a participant in Plaintiffs' and Class Members' communications about their Sensitive Information on the Website, because it used its participation in these communications to improperly share Plaintiffs' and Class Members' Sensitive Information with Google, TrafficJunky and third-parties that did not participate in these communications, that Plaintiffs and Class Members did not know were receiving their Sensitive Information, and that Plaintiffs and Class Members did not consent to receive their Sensitive Information.

185. As such, Defendants cannot viably claim any exception to ECPA liability.

186. Plaintiffs and Class Members have suffered damages as a direct and proximate result of Defendants' invasion of privacy in that:

- a. Learning that Defendants has intruded upon, intercepted, transmitted, shared, and used their Sensitive Information for commercial purposes has caused Plaintiffs and Class Members to suffer emotional distress;
- b. Defendants received substantial financial benefits from its use of Plaintiffs' and Class Members' Sensitive Information without providing any value or benefit to Plaintiffs or Class Members;
- c. Defendants received substantial, quantifiable value from its use of Plaintiffs' and Class Members' Sensitive Information, such as understanding how people use the Website and determining what ads people see on the Website, without providing any value or benefit to Plaintiffs or Class Members;

1 d. The diminution in value of Plaintiffs' and Class Members'
2 Sensitive Information and/or the loss of privacy due to Defendants
3 making such Sensitive Information, which Plaintiffs and Class
4 Members intended to remain private, no longer private.

5 187. Defendants intentionally used the wire or electronic communications to
6 increase its profit margins. Defendants specifically used the Pixels to track and utilize
7 Plaintiffs' and Class Members' Sensitive Information for financial gain.

8 188. Defendants were not acting under color of law to intercept Plaintiffs' and
9 the Class Members' wire or electronic communication.

10 189. Plaintiffs and Class Members did not authorize Defendants to acquire the
11 content of their communications for purposes of invading their privacy via the Pixels.

12 190. Any purported consent that Defendants may claim to have received from
13 Plaintiffs and Class Members was not valid.

14 191. In sending and acquiring the content of Plaintiffs' and Class Members'
15 communications relating to the browsing of The Website, Defendants' purpose was
16 tortious, criminal, and designed to violate federal and state legal provisions including a
17 knowing intrusion into a private, place, conversation, or matter that would be highly
18 offensive to a reasonable person.

19 192. As a result of Defendants' violation of the ECPA, Plaintiffs and the Class
20 are entitled to all damages available under 18 U.S.C. § 2520, including statutory damages
21 of whichever is the greater of \$100 a day for each day of violation or \$10,000, equitable
22 or declaratory relief, compensatory and punitive damages, and attorney's fees and costs.

COUNT VII
VIOLATIONS OF NEW YORK GENERAL BUSINESS LAW – DECEPTIVE
ACTS OR PRACTICES
N.Y. Gen. Bus. Law § 349
(On Behalf of Plaintiff C.P. and the Nationwide Class)

193. Plaintiffs repeat and reallege the allegations contained in paragraphs 1 through 192 as if fully set forth herein.

194. N.Y. Gen. Bus. Law § 349 prohibits use of “[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service[.]”

195. Defendants violated N.Y. Gen. Bus. Law § 349 by:

- a. Using the Tracking Tools to record and transmit the sensitive communications made by and to Plaintiff M.S. and New York Class Members through the Website with third parties, including Google, without their knowledge of consent; and
- b. Disclosing the sensitive communications made by and to Plaintiff M.S. and New York Class Members through the Website to third parties, including Google and TrafficJunky, in exchange for marketing and advertising services.

196. Defendants intended to mislead Plaintiff M.S. and New York Class Members and intended to induce Plaintiff M.S. and New York Class Members to rely on its misrepresentations and omissions.

197. As a result of Defendants’ violation of N.Y. Gen. Bus. Law. § 349, Plaintiff M.S. and New York Class Members are entitled to actual damages, treble damages, and attorneys’ fees, filing fees, and costs.

COUNT VIII
VIOLATIONS OF THE CALIFORNIA INVASION OF PRIVACY ACT
(“CIPA”)
Cal. Pen. Code § 360, et seq.
(On Behalf of Plaintiff M.S. and the California Subclass)

198. Plaintiffs repeat and reallege the allegations contained in paragraphs 1 through 197 as if fully set forth herein.

199. The California Legislature enacted CIPA in response to “advances in science and technology” that “have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications[.]” recognizing that “the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.” Cal. Pen. Code. § 630.

200. Under CIPA, it is unlawful to:

- a. “[W]illfully and *without the consent of all parties to the communication*, or in any unauthorized manner, read[], or attempt[] to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state;” or
- b. “[U]se, or attempt[] to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained[;]” or
- c. [A]id, agree[] with, employ[], or conspire[] with any person or persons to unlawfully do, or permit, or cause to be done any of the acts [prohibited by CIPA.]”

Cal. Penal Code § 631(a) (emphasis added).

1 201. At all relevant times, Defendants aided, employed, agreed with, and
2 conspired with Google and TrafficJunky, and likely other third parties, to track and
3 intercept Plaintiff M.S.’s and the California Subclass Members’ internet communications
4 while using the Website, specifically by installing and configuring the Tracking Tools to
5 permit Google and TrafficJunky to eavesdrop on and intercept in real-time the content of
6 intercept Plaintiff M.S.’s and the California Subclass Members’ private communications
7 with Defendants.

8 202. The content of those conversations included Sensitive Information,
9 including loan application determinations. Through Defendants’ installation and
10 configuration of the Tracking Tools on the Website, these communications were
11 intercepted by Google and TrafficJunky during the communications and without the
12 knowledge, authorization, or consent of Plaintiff M.S. and the California Subclass
13 Members.

14 203. Defendants intentionally inserted an electronic device into their Website
15 that, without the knowledge and consent of Plaintiff M.S. and California Subclass
16 Members, transmitted the substance of their confidential communications with
17 Defendants to third parties.

18 204. Defendants willingly facilitated Google, TrafficJunky and other third
19 parties’ interception and collection of Plaintiff M.S.’s and California Subclass Members’
20 Sensitive Information by embedding the Tracking Tools on the Website, thereby assisting
21 Google and TrafficJunky’s eavesdropping

22 205. The following items constitute “machine[s], instrument[s], or
23 contrivance[s]” under the CIPA, and even if they do not, the Tracking Tools falls under
24 the broad catch-all category of “any other manner”:

- 25 a. The computer codes and programs Google, TrafficJunky and other third
26 parties used to track intercept Plaintiff M.S.’s and the California

1 Subclass Members' communications while they were navigating the
2 Website;

3 b. Plaintiff M.S.'s and the California Subclass Members' internet
4 browsers;

5 c. Plaintiff M.S.'s and the California Subclass Members' computing and
6 mobile devices;

7 d. Defendants' and Google's web and ad servers;

8 e. The computer codes and programs used by Defendants', Google, and
9 other third parties to effectuate their tracking and interception of
10 Plaintiff M.S.'s and the California Subclass Members' communications
11 while they were using a browser to visit the Website; and

12 206. As demonstrated hereinabove, Defendants violate CIPA by aiding and
13 permitting third parties, including Google and their agents, employees, and contractors to
14 receive Plaintiff M.S.'s and the California Subclass Members' Sensitive Information in
15 real time through the Website without their consent

16 207. By disclosing Plaintiff M.S.'s and the California Subclass Members'
17 Sensitive information, Defendants violated Plaintiff M.S.'s and California Subclass
18 Members' statutorily protected right to privacy.

19 208. As a result of Defendants' violation of the CIPA, Plaintiff M.S. and the
20 California Subclass Members are entitled to treble actual damages related to their loss of
21 privacy in an amount to be determined at trial, statutory damages, attorney's fees,
22 litigation costs, injunctive and declaratory relief, and punitive damages.

23
24 **COUNT IX**
VIOLATIONS OF THE CALIFORNIA UNFAIR COMPETITION LAW
("UCL")

25 **Cal. Bus. & Prof. Code, § 17200, et seq.**
26 **(On Behalf of Plaintiff M.S. and the California Subclass)**

209. Plaintiffs repeat and reallege the allegations contained in paragraphs 1 through 208 as if fully set forth herein.

210. The UCL prohibits any “unlawful, unfair or fraudulent business act or practice” and any “unfair, deceptive, untrue or misleading advertising.” Cal. Bus. & Prof. Code, § 17200.

211. Defendants violated the “unlawful” prong of the UCL by violating Plaintiff M.S.’s and California Subclass Members’ right to privacy, as well as by violating the statutory counts alleged herein.

212. Defendants violated the unfair prong of the UCL by:

- a. Using the Tracking Technologies to record and transmit the sensitive communications made by and to Plaintiff M.S. and the California Subclass Members through the Website with third parties, including Google and TrafficJunky, without their knowledge or consent; and
- b. Disclosing the sensitive communications made by and to Plaintiff M.S. and the California Subclass Members through the Website to third parties, including Google and TrafficJunky, in exchange for marketing and advertising services.

213. As a result of Defendants’ violations of the UCL, Plaintiff M.S. and the California Subclass Members have suffered the diminution of the value of their Sensitive Information, as alleged above.

214. As a result of Defendants’ violation of the UCL, Plaintiff M.S. and the California Subclass Members are entitled to injunctive relief, as well as restitution necessary to restore to them in interest any money or property, real or personal, acquired through Defendants’ unfair competition practices.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of other Class Members, pray for judgment against Defendants as follows:

- A. an Order certifying the Nationwide Class, and California and New York Subclasses, and appointing the Plaintiffs and their Counsel to represent the Classes;
- B. equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Sensitive Information of Plaintiffs and Class Members;
- C. injunctive relief requested by Plaintiffs, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members;
- D. an award of all damages available at equity or law, including, but not limited to, actual, consequential, punitive, statutory and nominal damages, as allowed by law in an amount to be determined;
- E. an award of attorney fees, costs, and litigation expenses, as allowed by law;
- F. prejudgment interest on all amounts awarded; and
- G. all such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and other members of the proposed Classes, hereby demand a jury trial on all issues so triable

Dated: August 13, 2025

Respectfully submitted,

1 Michael Connett
2 mconnett@sirillp.com
3 **SIRI & GLIMSTAD LLP**
4 700 S. Flower Street, Ste. 1000
5 Los Angeles, CA 90017
6 Telephone: (772) 783-8436

7
8 *Signatures Continue on Following*
9 *Page*

10 Tyler J. Bean*
11 Sonjay C. Singh*
12 **SIRI & GLIMSTAD LLP**
13 745 Fifth Avenue, Suite 500
14 New York, New York 10151
15 Tel: (212) 532-1091
16 E: tbean@sirillp.com
17 E: ssingh@sirillp.com

18 **pro hac vice*

19 *Attorneys for Plaintiffs and the*
20 *Class*